A Fast Algorithm for Rational Normal Curves

Josef Schicho, RICAM, Austrian Academy of Sciences

Extended Abstract

A rational normal curve is an irreducible projective curve $C \subset \mathbb{P}^d$ of degree d not contain in a hyperplane. If C is defined over some coefficient field k and also has a point over k, then there exists a projective transformation defined over k transforming C to the image C_0 of the parametrization

$$p : \mathbb{P}1 \to \mathbb{P}^n, (s : t) \mapsto (s^d{:}s^{d-1}t{:}\ldots{:}t^d).$$

For a given rational curve C, the following three problems are algorithmically equivalent (i.e. we have fast algorithms reducing any of them to any of them):

1. to find a transformation of C to the standard form C_0 above;
2. to find a rational parametrization of C;
3. to find a rational point on C.

The second problem appears as a subproblem of the various algorithms for parametrizing curves of genus zero (see M. C. Harrison's implementation in Magma), and as a subproblem for an algorithm for reparametrizing an algebraic curve over a smaller field (see [1]), and as a subproblem for computing normal forms for hyperelliptic curves (see the algorithm of M. van Hoeij implemented in Maple). In all three cases, this subproblem constitutes a computational bottleneck. It is therefore desirable to have a fast algorithm for it.

The Lie algebra method has been introduced by W. de Graaf, M. C. Harrison, J. Pílnikov'a and the author for solving the parametrization problem for Del Pezzo surfaces (see [3]). The Lie algebra of a projective variety X is defined via the Lie group of linear automorphisms of X. For many varieties, it is not very interesting because there are not enough automorphisms. But in the case of Del Pezzo surfaces of degree at least 6, the Lie algebra can be used for computing a parametrization.

Here we apply the Lie algebra method to a rational normal curve of degree d given by a set of generators for its vanishing ideal (not necessarily a Gröbner basis). We first compute the Lie algebra of C by solving a linear system of equations in $\mathcal{O}(d^2)$ unknowns. Then we compute a Chevalley basis and its weight vectors, and this will solve the first problem in the list above.

If d is odd, then the computation of the Chevalley basis requires only solving linear systems $\mathcal{O}(d)$ unknowns, which is faster then the computation of the

Lie algebra. If d is even, then it is necessary to find a k-rational point on a conic. If $k = \mathbb{Q}$, then the complexity of this problem can be compared with the complexity of factorization of integers. It is well-known that this step cannot be avoided in general.

We implemented the algorithm in Magma [2] and compared with the already existing algorithm ParametrizeRationalNormalCurve, which has been implemented by M. C. Harrison and is based on an algorithm by F.-O. Schreyer using syzygy computations. In the examples tested so far, the comparison does not show a clear advantage of our implementation; but the statistics does reflect the polynomial complexity in the odd degree case.

References

[1] C. Andradas, T. Recio, and R. Sendra. Base field restriction techniques for parametric curves. In *Proc. ISSAC 1997*. ACM Press, 1999.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24:235–265, 1997.

[3] W. A. de Graaf, M. Harrison, J. Píniková, and J. Schicho. A Lie algebra method for the parametrization of Severi-Brauer surfaces. *J. Algebra*, 303, 2006.